Daily Open Source Infrastructure Report
1 May 2012

Top Stories

- Workers used mud to plug a well in eastern Wyoming, April 27, ending a 3-day eruption of potentially explosive natural gas that forced 50 people from their homes. – *Associated Press* (See item **1**)
- Tornadoes disabled a power station, damaged homes, and downed power lines making many roads impassable in southeastern Colorado, authorities said. – *United Press International* (See item **3**)
- Hackers stole about 40 gigabytes worth of files with data including locations of U.S. Army Reserve facilities and communication company codes, from the Lake County Sheriff's Office in Florida. – *Softpedia* (See item **40**)
- Mission-critical routers used to control critical infrastructure are being updated by the manufacturer, RuggedCom, to remove a backdoor that can allow malicious actors to hijack the devices. – *Ars Technica* (See item **48**)
- St. Louis officials were expected to more closely scrutinize large tents commonly set up near downtown stadiums after one collapsed in high winds, killing one person and injuring dozens of others. – *Associated Press* (See item **53**)

Fast Jump Menu

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: LOW, Cyber: LOW
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) - [http://www.esisac.com]

1. *April 30, Associated Press* – (Wyoming) **Chesapeake Energy plugs blown oil well leaking gas.** Workers at a blown Chesapeake Energy Corp. oil well in eastern Wyoming took advantage of changing winds April 27 to plug the well with mud and end a powerful, 3-day eruption of potentially explosive natural gas. The blowout of methane gas happened April 24 at the drilling site 5 miles northeast of Douglas. The operation to stem the air pollution and the flow of gas — not to mention risk of an explosion that could destroy a multimillion-dollar drilling rig — took about 90 minutes, according to the supervisor of the Wyoming Oil and Gas Conservation Commission. Workers continued to pump mud down the well, which Oklahoma City-based Chesapeake Energy recently drilled more than 3 miles vertically and horizontally under the rolling prairie. The blowout first occurred April 24, pushing drilling mud to the surface. Clouds of gas blurred the horizon. Authorities issued an evacuation advisory to 67 people in homes within 2.5 miles of the well, and 50 people heeded it.
Source: http://www.chem.info/News/2012/04/Safety-Chesapeake-Energy-Plugs-Blown-Oil-Well-Leaking-Gas/

2. *April 30, Associated Press* – (Kentucky) **MSHA cites 214 violations in March at 9 coal mines.** The Mine Safety and Health Administration (MSHA) issued 214 violations during special inspections at 9 coal mines in March, the Associated Press reported April 30. Inspectors closed Redhawk Mining's Redhawk No. 1 in Floyd County, Kentucky, for 72 hours and issued 40 violations. It has a history of releasing methane and was on notice about ventilation. Yet the MSHA says there was insufficient air flow, and water sprayers that control dust were not working properly. The MSHA also issued 38 citations and 16 unwarrantable failure orders at Perry County Coal's E3-1 Mine in Kentucky. Inspectors found 14 accumulations of explosive material, from

paper-thin coatings of coal dust to piles of coal 3 feet thick. The MSHA said the hazards had clearly existed for some time. The impact inspections began in 2010, after West Virginia's Upper Big Branch mine disaster.
Source: http://www.kentucky.com/2012/04/30/2170001/msha-cites-214-violations-in-march.html#wgt=rcntnews

3. *April 27, United Press International* – (Colorado) **Tornadoes heavily damage SE Colorado.** Tornadoes heavily damaged homes, disabled a power station, and downed power lines April 27 in southeastern Colorado, authorities said. The Wiley fire chief said the tornadoes were reported south of Lamar, north of Lamar, and near Chivington, but they were not confirmed, KUSA 9 Denver reported. Colorado Emergency Management officials urged people in the Lamar area to exercise caution because of downed power lines. In a statement, the agency said power was knocked out in Lamar, Eads, Chivington, Sheridan Lake, and surrounding areas. The Colorado State Patrol said in a news release tornadoes caused "severe property damage" in the Lamar area, where the power station was disabled. Gas stations in Lamar could not pump fuel, the State Patrol said, urging motorists to avoid Lamar until power was restored.
Source: http://www.disasternews.net/news/article.php?articleid=4596

For another story, see item **9**

[Return to top]

Chemical Industry Sector

4. *April 29, Associated Press* – (Missouri) **Kansas agency reaches tentative agreement with DuPont.** State and federal authorities reached a tentative agreement that would require DuPont to pay more than $250,000 for pollution in Kansas, the Associated Press reported April 29. The Kansas Department of Health and Environment and the U.S. Department of the Interior accused the Delaware-based chemical company of violating the Clean Water Act with pollution from mining in Cherokee County. The federal complaint filed April 19 said the pollution from the Waco sub site left high levels of lead, cadmium, and zinc in soil and groundwater. If approved, the proposed consent decree would require DuPont to pay $252,739 for cleanup and damages. The Cherokee County site was a federal Superfund site for decades. The 560-acre Waco section is about 11 miles south of Pittsburg, a heavy mining area.
Source: http://www.ksdk.com/news/article/318148/28/Kansas-agency-reaches-tentative-agreement-with-DuPont-

For more stories, see items **9** and **15**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

See item **30**

[Return to top]

Critical Manufacturing Sector

See item **48**

[Return to top]

Defense Industrial Base Sector

See item **48**

[Return to top]

Banking and Finance Sector

5. *April 30, Help Net Security* – (International) **Phishing email targets Santander clients.** Customers of Santander, one of the largest banking groups in the world, are currently being targeted with a phishing e-mail masquerading as a bogus notification of a scheduled software upgrade. According to Hoax-Slayer, the offered link takes users to a spoofed Santander online banking Web site, where they are asked to enter their ID, passcode, customer PIN, mobile number, landline number, and date of birth. Having done that, the site requests users to set up three security questions and answers, which are then misused by the phishers to gain access to the users' account. In the end, users are redirected to the legitimate Web site of Santander's United Kingdom branch in order to maintain the illusion that nothing out of the ordinary happened.
Source: http://www.net-security.org/secworld.php?id=12834

6. *April 28, Associated Press* – (Pennsylvania; Arizona) **Six men charged in alleged $10 million finance scam.** Federal grand jurors in Philadelphia indicted six businessmen on charges they defrauded hundreds of hopeful entrepreneurs out of millions of dollars. The indictment made public April 27 alleged the men associated with Remington Financial Group bilked at least 800 people seeking funds for commercial ventures. According to the grand jury, victims paid thousands of dollars in up-front fees to Remington based on false representations that the company found investors for their projects. Prosecutors said victims collectively lost more than $10 million between 2005 and 2011. The company, which was later renamed Remington Capital, had offices in Arizona and Pennsylvania. Remington's founder was listed among the defendants. He faces charges including fraud and money laundering.
Source: http://www.whptv.com/news/local/story/Six-men-charged-in-alleged-10-million-finance-scam/zuCilQFnPU61g-cW3pmDEw.cspx

7. *April 27, Chicago Tribune* – (Illinois) **6 charged in skimming scheme at restaurants, Wrigley Field.** Six people were accused of stealing bank information from patrons at Chicago restaurants and Wrigley Field, then running up more than $200,000 in purchases on phony cards, the Chicago Tribune reported April 27. A man allegedly paid employees to skim credit card information by using a credit card reader he provided, according to the State attorney general's office. The employees would swipe the cards and the man would create counterfeit cards to charge up thousands of dollars in purchases, the office said. The employees worked at Wrigley Field, RL Restaurant, Taco Bell, and McDonald's, officials said. Two defendants were charged with using the phony cards to make illegal purchases, officials said. The suspects, all from Chicago, were each charged with one count of conspiracy to commit a financial crime. Four defendants were also charged with continuing a financial crimes enterprise. Three defendants face an additional identity theft charge. Officials said the bank accounts that were compromised include Chase, U.S. Bank, Citibank, Harris Bank, American Express, Bank of America, and Fifth Third Bank.
Source: http://articles.chicagotribune.com/2012-04-27/news/chi-6-charged-in-skimming-scheme-at-wrigley-and-chicago-restaurants-20120427_1_credit-card-wrigley-field-counterfeit-cards

8. *April 27, WEWS 5 Cleveland* – (National) **New email claims to be from FDIC, threatens users confidential and personal data.** A fraudulent e-mail offering cash in return for survey information could obtain access to personal and confidential data, WEWS 5 Cleveland reported April 27. The Federal Deposit Insurance Corporation (FDIC) issued a warning to computer users that it received numerous reports of fraudulent e-mails that have the appearance of having been sent by the FDIC. The e-mail contains a subject line "Survey Code: STJSPNUPUT." It reads "you have been chosen by the FDIC to take part in our quick and easy 5 question survey. In response, will credit $100 dollars to your account just for your time." The FDIC is warning consumers not to click on the link provided in the e-mail, as it is intended to obtain personal information or load malicious software onto users' computers. The FDIC reminds consumers that it does not send unsolicited e-mail to consumers or business account holders.
Source: http://www.newsnet5.com/dpp/news/local_news/investigations/new-email-claims-to-be-from-fdic-threatens-users-confidential-and-personal-data

[Return to top]

Transportation Sector

9. *April 30, KGNB 1420 AM New Braunfels* – (Texas) **Tanker filled with flammable chemical teeters at local gas station; NBFD/Haz-Mat Team spend hours correcting the situation.** A potentially dangerous HAZMAT situation in New Braunfels, Texas, took more than 7.5 hours to safely defuse April 27 and April 28. Firefighters were called out to the Pilot Truck Stop on Loop 337 at I-35 April 27 after the driver of an 18-wheeler tried to unhitch his cargo but had problems with the truck's jack. While unhitching the tanker from the cab, the jack punctured the asphalt, causing the tanker to teeter on 2 wheels, and causing it to lean against a second 18-wheeler. The tanker truck

was carrying about 43,000 pounds of a highly flammable chemical called tritherm that if spilled or leaked would require a 0.5-mile area to be evacuated. Fortunately, none of the chemical leaked during the initial incident, but a HAZMAT company helped make sure there was not a leak while trying to right the tanker. The Pilot gas station, store, and surrounding parking lot were still evacuated as a precaution.
Source: http://kgnb.am/news/tanker-filled-flammable-chemical-teeters-local-gas-station-nbfdhaz-mat-team-spend-hours-correct

10. *April 30, Contra Costa Times* – (California) **I-680 in Pleasanton cleared after rig crash causes lengthy overnight blockage.** Interstate 680 near Bernal Avenue in Pleasanton, California, was cleared after an April 29 rig crash sent chunks of concrete onto the roadway and prompted a 9-hour road closure, the California Highway Patrol said April 30. A southbound big rig lost control and hit the center divider, causing it to turn onto its side and breaking off parts of the concrete barrier, which landed in the northbound lanes. The rig driver suffered minor injuries. A HAZMAT crew was sent to the incident because the rig's load contained volatile chemicals. They were not released in the crash. Crews did have to clean up diesel fuel that spilled. Authorities closed all directions of the freeway near the crash site to clean up the roadway. They phased in lane openings throughout the night and gave an all-clear early the next morning.
Source: http://www.mercurynews.com/news/ci_20513009/big-rig-accident-closes-both-directions-i-680?source=rss

11. *April 28, Associated Press* – (Texas) **13 injured in Texas crash involving school bus.** Nine students were among 13 hospitalized after a fiery 4-vehicle crash that left a charred school bus on its roof near Seguin, Texas, the Associated Press reported April 28. A school official said none of the middle and high school students suffered life-threatening injuries in the April 27 crash. The driver of an 18-wheeler was airlifted to a San Antonio hospital but was expected to survive. A Seguin Independent School District spokesman said the bus was new and designed to cushion the impact of head-on collisions. A Texas Department of Public Safety trooper said the accident began when the 18-wheeler clipped a car that moved to the shoulder to let it pass.
Source: http://lubbockonline.com/texas/2012-04-28/13-injured-texas-crash-involving-school-bus#.T56qpNlKWF9

12. *April 27, Associated Press* – (New Jersey) **Baby security breach closes NJ airport terminal.** A terminal at New Jersey's Newark Liberty International Airport was shut down for over an hour, April 27, after officials discovered that a baby was not properly screened, Transportation Security Administration officials said. The Port Authority of New York and New Jersey, which operates the airport, described the incident as a security breach that occurred at a security checkpoint. Terminal C was evacuated and passengers had to go through security screening again.
Source: http://www.valleynewslive.com/story/17861097/baby-security-breach-closes-nj-airport-terminal

For more stories, see items **3**, **13**, **28**, and **48**

[Return to top]

Postal and Shipping Sector

13. *April 29, WITI 6 Milwaukee* – (Wisconsin) **Man in custody for placing suspicious envelope in mailbox on east side.** Milwaukee police shut down streets on the lower east side to investigate a suspicious package April 28. Police said a man recorded himself putting a letter he said was laced with anthrax in a mailbox before notifying several media outlets. As it turns out, the letter was a hoax and the man was taken into custody. Knapp Street was closed for nearly 3 hours as police responded to an e-mail they received alerting them to a dangerous package in the area. A video showed the man, with a woman by his side, speaking nonsense, placing a letter addressed to the Wisconsin Department of Workforce Development in the mail on Milwaukee's lower east side. The man then sent an e-mail to various Milwaukee media outlets saying, "There is a letter laced with Anthrax at East Knapp Street," with a link to the video.
Source: http://fox6now.com/2012/04/29/milwaukee-police-investigate-suspicious-package-on-knapp-st/

14. *April 27, Associated Press* – (Arizona) **USPS probes mailbox damage, theft in Mohave County.** Federal authorities were investigating damages to mailboxes and mail theft in Mohave County, Arizona, the Associated Press reported April 27. U.S. Postal Service (USPS) employees found 6 large neighborhood distribution cluster box units plus some 30 individual rural mail boxes broken into and their contents removed April 26. Authorities said there are possibly 150 mail theft victims. All of the affected customers were notified, and the USPS is working to repair the damaged cluster boxes. Mohave County sheriff's investigators and the U.S. Postal Inspection Service ware actively working the case.
Source: http://ktar.com/6/1534310/USPS-probes-mailbox-damage-theft-in-Mohave-County

[Return to top]

Agriculture and Food Sector

15. *April 30, Rochester Democrat and Chronicle* – (New York) **OSHA cites Upstate Niagara Milk Coop for safety violations.** Federal work-safety regulators cited Upstate Niagara Milk Cooperative's Rochester, New York plant, suggesting fines of $200,500 for 12 violations, most of which revolve around safeguards on the ammonia used in refrigeration, the Rochester Democrat and Chronicle reported April 30. The citations from the Occupational Safety and Health Administration (OSHA) range from blocking an entrance to the height of venting pipe, to lack or adequacy of certain procedures for workers in confined places, including inside dairy tanks. Some of the violations are repeats of ones cited and addressed at another Upstate plant in Buffalo. The assistant area director for the OSHA said the venting pipe needed to be taller so a potential discharge would not harm workers.
Source:
http://www.democratandchronicle.com/article/20120430/BUSINESS/304240063/Upstate-Niagara-Milk-Cooperative-OSHA

16. *April 30, Agence France-Presse* – (International) **China shuts down Coca-Cola plant over chlorine contamination, government says.** Authorities in northern China ordered a Coca-Cola bottling plant to shut after finding its products were contaminated by chlorine, according to a government statement. Shanxi province ordered an investigation after media reports that a batch of drinks contained water with higher levels of chlorine, the province's quality bureau said the weekend of April 28. The contamination occurred in February when water with small amounts of chlorine accidentally flowed into water used for drinks during maintenance work, the official Xinhua news agency said April 29. Xinhua quoted the Shanxi plant as saying its products were safe and did not present a threat to human health.
Source: http://www.myfoxdfw.com/story/17927813/china-shuts-down-coca-cola-plant-over-chlorine-contamination-government-says

17. *April 30, Sturgis Journal* – (Michigan) **Bronson fire kills 1,000 pigs.** A massive fire in Bronson, Michigan, April 28 killed at least 1,000 pigs and damaged 3 barns. First arriving personnel found 3, 40 by 120 foot barns on fire. Two of the barns were a complete loss, while the other suffered smoke and water damage. Authorities said 1,000 pigs perished in the fire. Firefighters were able to save about 200 pigs. Authorities estimated damage of $350,000 to the buildings and another $200,000 to contents.
Source: http://www.sturgisjournal.com/topstories/x1018070704/Bronson-Fire-kills-1-000-pigs

18. *April 30, Buncombe County Department of Health* – (North Carolina) **Buncombe County - cases of Salmonella Paratyphi B increase.** The Buncombe County Department of Health in North Carolina, reported 5 more cases of Salmonella Paratyphi B were identified over the weekend of April 28, bringing the total to 34, as of April 30. The local health department is working with the North Carolina Department of Public Health, Center for Disease Control, U.S. Department of Agriculture, and others to continue intensive testing, interviewing, and epidemiological investigation of the outbreak to stop the spread of the disease. Cases still appear to have been associated with residence or travel to Buncombe County since February 28. A single source of infection was not confirmed. State and local health officials do not have final laboratory test results that would allow conclusive identification of a specific source of salmonella contamination. The health director said that at this point in the investigation, it is better to broadly implement control measures than to speculate or falsely identify a source. Based on the preliminary lab findings, control measures were issued to food establishments in Buncombe County by environmental health specialists. The Asheville Independent Restaurant Association voluntarily worked with the health department to educate food workers and heighten awareness of ways to prevent the spread of disease.
Source: http://www.buncombecounty.org/common/health/Salmonella4-30-12.pdf

19. *April 29, Portland Press Herald* – (Maine) **Investigator: Sickened Maine horses difficult to treat.** Maine's State veterinarian was working to find the source of a rare botulism outbreak that was believed to have killed 23 horses at the Whistlin' Willows Farm in Gorham in April, the Portland Press Herald reported April 29. The state veterinarian said there are no signs the animals were cared for improperly. Part of the

problem during an outbreak, said the veterinarian, is once a horse exhibits signs of botulism poisoning, there is little veterinarians can do to treat the animal. State inspectors believe the powerful and fast-acting neurotoxin responsible for the outbreak developed in bales of silage, which is packaged in white plastic while the grass is still moist, unlike hay, which is dried. A horse can die from botulism within hours of ingestion. The veterinarian said that because botulism is so rare, Maine horse owners do not commonly vaccinate their animals against it.
Source: http://www.pressherald.com/news/investigator-sickened-horses-difficult-to-treat_2012-04-29.html

20. *April 28, Food Safety News* – (Maryland; Virginia; Washington, D.C.) **Soybean sprouts recalled due to Listeria.** Soybean Sprouts from Henry's Farm Inc. of Woodford, Virginia, were recalled because of possible Listeria monocytogenes contamination, according to the Virginia Department of Agriculture and Consumer Services, Food Safety News reported April 28. The following products were recalled: 1.5-pound clear plastic bags of Grown in Natural Spring Water Soybean Sprouts and bulk, about 10-pound plastic bags of Soybean Sprouts. The items were distributed to retail stores in Virginia, Maryland, and Washington, D.C.
Source: http://www.foodsafetynews.com/2012/04/soybean-sprouts-recalled-due-to-listeria-risk/

21. *April 28, Lebanon Daily News* – (Pennsylvania) **Sow, 10 piglets perish in hog barn fire.** A sow and 10 piglets died in a hog farm fire in East Hanover Township, Pennsylvania, April 28. "It was confined to two rooms and part of a hallway," the Ono fire chief said. The barn was about 75 feet by 350 feet long. A preliminary investigation indicated the fire was probably caused by an electrical malfunction, the chief said. He estimated the damage was between $75,000 to $100,000. Units were on the scene about 3 hours. Eight other agencies assisted Ono in fighting the fire.
Source: http://www.ldnews.com/lebanonnews/ci_20503757/sow-10-piglets-perish-hog-barn-fire

22. *April 27, Food Safety News* – (National) **Diamond Pet Foods expands dry dog food recall.** Diamond Pet Foods expanded a recall, announced April 6, for certain batches of Diamond Natural Lamb Meal & Rice dry dog food, to include one production run and four production codes of Chicken Soup for the Pet Lover's Soul Adult Light formula dry dog food. One bag tested positive for Salmonella, and the company said the recall of the four production codes was a precautionary measure, Food Safety News reported April 27. The latest recall is for: Chicken Soup for the Pet Lover's Soul Adult Light Formula dry dog food in 35-pound bags and Chicken Soup for the Pet Lover's Soul Adult Light Formula dry dog food in 6-pound bags. The dog food was distributed in Florida, Kentucky, Massachusetts, Michigan, New York, North Carolina, Ohio, Pennsylvania, South Carolina, and Virginia, and may have been further distributed to other states, through pet food channels. Diamond Pet said it is working directly with distributors and retailers who carry the products to remove them from the supply chain.
Source: http://www.foodsafetynews.com/2012/04/diamond-pet-foods-expands-dry-dog-food-recall/

23. *April 27, Orangeburg Times and Democrat* – (South Carolina) **Irrigation irritation: Recent thefts leave farms' water systems high and dry.** Orangeburg County, South Carolina police officers were looking for a Moncks Corner man after a Eutawville farm's irrigation system was damaged April 24, apparently in an attempt to steal copper wire. Another man was taken into custody April 25 for his part in the damage at the Harvest Court farm. He was charged with malicious injury to personal property of $10,000 or more, grand larceny, and conspiracy. "We are monitoring farms and irrigation systems since these have been the primary targets of copper theft over the past several months," said the sheriff. At about the same time across the county, thieves were plundering another system at Carolina Fresh Farms near Norway. A spokesman for the property said the system suffered about $4,000 in damages. He said over the last 2 years, copper thieves have cost him $60,000 for repairs to 6 irrigation systems. That does not count the crop loss from lack of water. A Clemson extension agent said some farmers are installing cameras and other security systems that alert a farmer through his or her cell phone.
Source: http://thetandd.com/news/local/irrigation-irritation-recent-thefts-leave-farms-water-systems-high-and/article_fd41c8dc-8ffd-11e1-816c-0019bb2963f4.html

For another story, see item **56**

[Return to top]

Water Sector

24. *April 30, New York Post* – (New York) **Divers deep-fix city link to water.** Deep-sea divers completed repairs on New York City's main water-supply system after 35 days of work, the New York Post reported April 30. The repairs on the system based in Dutchess County were needed after it sprung a 20-million-gallon-a-day leak. The process was lengthy because divers had to take turns going down nearly 700 feet deep to twist wrenches, take measurements, and operate heavy equipment to replace a plug in an underwater shaft that connects the city's water supply to an upstate reservoir system. In between shifts, they spent down time in a chamber that mimics the atmospheric pressure of being underwater. The plug installation was the first stage of a $2.1 billion initiative to drain the shaft and build a bypass tunnel around a leaking section of the 85-mile Delaware Aqueduct, which supplies roughly half of the city's drinking water.
Source:
http://www.nypost.com/p/news/local/divers_deep_fix_city_link_to_water_PkAoEXHJuR12hUVmoB6Y0N?utm_medium=rss&utm_content=Local

25. *April 30, U.S. Geological Survey* – (National) **From decade to decade: What's the status of our groundwater quality?** There was no change in concentrations of chloride, dissolved solids, or nitrate in groundwater for more than 50 percent of well networks sampled in an analysis released April 30 by the U.S. Geological Survey (USGS) that compared samples from 1988 to 2000 to samples from 2001 to 2010. For those networks that did have a change, seven times more networks saw increases as opposed to decreases. The analysis was done by the USGS National Water Quality

Assessment Program (NAWQA) to determine if concentrations of these constituents have increased or decreased significantly from the 1990's to the early 2000's. Though chloride, nitrate, and dissolved solids occur naturally, human activities can cause concentrations to exceed natural levels. At high concentrations, these chemicals can have adverse effects on human and environmental health. The report, "Methods for Evaluating Temporal Groundwater Quality Data and Results of Decadal-Scale Changes in Chloride, Dissolved Solids, and Nitrate Concentrations in Groundwater in the United States, 1988-2010" as well as links to interactive maps showing long-term groundwater trends, can be found on the USGS's Web site.
Source: http://www.usgs.gov/newsroom/article.asp?ID=3189#.T565ZdlYtnM

26. *April 30, WALB 10 Albany* – (Georgia) **Valdosta water restriction could be lifted Tuesday.** The temporary water restriction in Valdosta, Georgia, could be lifted May 1, WALB 10 Albany reported April 30. City officials said they replaced water pumps and a second temporary water pump was expected to be put in place April 30. After the installation of the pump, the utility department planned to assess whether the restriction should continue. They expected to return to their even/odd watering schedule for outdoor irrigation once the restriction is lifted. While water levels were steady, city officials asked Valdosta residents to only use water when it is essential. They say citizens have cut back on water use since the restriction was put in place the week of April 23. City officials requested the cutback after severe vibrations in water pumps put the pumps out of commission.
Source: http://www.walb.com/story/17931780/valdosta-water-restriction-could-be-lifted-tuesday

27. *April 30, Mystic River Press* – (Connecticut) **Bill sent to gov.** The Connecticut House of Representatives approved legislation that establishes a process to inform the public whenever a sewage spill occurs, the Mystic River Press reported April 30. Sent to the governor for his consideration, the legislation requires the Connecticut Department of Energy and Environmental Protection (DEEP) to post information on unanticipated sewage spills on its Web site beginning in July 2014. The online notice will have details on the spill such as the date, time, volume, duration and steps taken to contain it, as well as public health or environmental concerns and any public safety precautions that should be taken. In July 2013, the DEEP must begin posting information on anticipated sewer overflows resulting from storm events. According to the U.S. Environmental Protection Agency, between 1.8 and 3.5 million Americans become ill annually from contact with recreational waters contaminated by sewage. Currently there is no federal law requiring public notification if a sewage overflow has contaminated a local beach or waterway or entered a community.
Source: http://www.thewesterlysun.com/mysticriverpress/news/rep-urban-bill-sent-to-gov/article_87c05576-8e16-11e1-9070-001a4bcf887a.html

28. *April 29, KNSD 7 San Diego* – (California) **Water main breaks on Morena Blvd.** A water main break in San Diego early April 29 left many residents without water. Police said it was unknown exactly how it happened. They set up barricades around the area. The San Diego Water Department confirmed a 16-inch cast iron water main broke and four blocks in the surrounding area were without water. Water department officials

expected the water to be shut off for most of April 29 so they could make repairs.
Source: http://www.nbcsandiego.com/news/local/Water-Main-Break-Morena-Blvd-149422575.html

29. *April 27, West Des Moines Patch* – (Iowa) **Waterworks well damaged by theft seeking copper.** An employee of West Des Moines Waterworks in Iowa, reported April 20 a well house was damaged, the West Des Moines Patch reported April 27. He said the damage occurred when a cable that leads from a communication tower to the well house was cut. Waterworks employees estimated the damage at $1,500. The suspect reportedly cut a 25-foot section of cable. The waterworks employee told a police officer the suspect might have been trying to steal copper. A computer shows information from the well house to the main waterworks facility was interrupted the morning of April 18.
Source: http://westdesmoines.patch.com/articles/waterworks-well-damaged-by-theft-seeking-copper

For more stories, see items **4**, **38**, and **54**

[Return to top]

Public Health and Healthcare Sector

30. *April 27, WFLD 32 Chicago* – (Illinois) **Hospitals prepare for NATO attack, perform dirty bomb response drills.** April 25, 10 Chicago-area hospitals performed drills simulating a radioactive dirty bomb explosion in preparation for a worst-case scenario during May's NATO summit. An estimated 500 medical professionals and other volunteers donned bulky protective suits, tested radiation detectors, and ministered to about 100 U.S. Navy recruit "victims." The Navy volunteers were posing as victims of a so-called "dirty bomb" that had exploded, leaving them with deadly radioactive cesium on their skin. Doctors and nurses would risk their own lives if they began treating the wounded before they are cleansed of radiation. The dirty bomb scenario was worked out in conjunction with the Secret Service and the DHS.
Source: http://www.myfoxchicago.com/dpp/news/metro/suburban-hospitals-prepare-for-nato-attack-perform-dirty-bomb-response-drills-20120426

31. *April 27, Pueblo Chieftan* – (Colorado) **Dozens stricken after center luncheon.** Colorado's Pueblo City-County Health Department was investigating the cause of what sickened 27 people following a luncheon for the Pueblo Community Health Center April 24. One possibility could be Norovirus, which more commonly is known as the stomach flu or viral gastroenteritis. The health center's chief foundation officer sent an e-mail to those who attended the dinner, alerting them to the outbreak and telling them they would be contacted by health officials. The e-mail was sent to several elected officials at the city and county levels, college leaders, doctors, and members of the medical community.
Source: http://www.chieftain.com/news/local/dozens-stricken-after-center-luncheon/article_d0a4f678-8ff8-11e1-821f-0019bb2963f4.html

32. *April 26, KHOU 11 Houston* – (Texas) **FBI raids Westbury Community Hospital system for suspicion of Medicare, Medicaid fraud.** FBI agents conducted three simultaneous raids at centers in the Westbury Community Center Hospital system April 26 in Houston, according to authorities. The hospitals are all part of the group formerly known as Continuum. Authorities were investigating to find out if the company was illegally billing Medicare and Medicaid. Officials were trying to figure out if the company was using ambulances or work vans to round up homeless people off the streets then take them to their facilities for treatment. Sources said patients might not be getting treatment at all; instead they watch television all day before being sent back to the streets. A hospital administrator denied that claim. The IRS, FBI, HPD, and other law enforcement agents questioned every employee. Meanwhile, some regular patients who receive treatment every day said they were turned away. Investigators hauled off boxes of evidence from the raids to see if the business was as it should be.
Source: http://www.khou.com/news/local/FBI-raids-Westbury-Community-Hospital-system-for-suspicion-of-Medicare-Medicaid-fraud-149106135.html

For another story, see item **18**

[Return to top]

Government Facilities Sector

33. *April 30, Help Net Security* – (New York; International) **Columbia University notifies employees of breach.** Personal and financial information of 3,000 current and former employees of Columbia University in New York City and 500 other individuals were available online from January 2010 to March 10, according to a breach notification sent out by the education institution the week of April 23. The file containing names, addresses, Social Security numbers, and bank account numbers (but not the names of the banks or the routing numbers) of the affected individuals ended up online after a programmer saved it by mistake on a public server, and Google indexed it. The file was pulled and deleted from Google's Index. Even though access logs for the file said it was not accessed by anyone while it was online, the university has promptly notified the victims about the matter, apologized, and offered a free 2-year subscription to a credit monitoring system to each of them.
Source: http://www.net-security.org/secworld.php?id=12837&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HelpNetSecurity+(Help+Net+Security)&utm_content=Google+Reader

34. *April 30, Associated Press* – (New York) **NY high school reopening after break-in, damage.** Classes resumed April 30 at a suburban Rochester, New York high school where a student was charged with causing tens of thousands of dollars in damage during a break-in the week of April 23. Officials at Brighton High School canceled classes April 27 after extensive damage to the building and science lab equipment was discovered by staff members. Police said a driver's education car was stolen from the school. Rochester media outlets reported police arrested a student and charged him with burglary, grand larceny, and criminal mischief. He is also charged with resisting arrest.

Source: http://www.wcax.com/story/17929256/ny-high-school-reopening-after-break-in-damage

35. *April 30, Greenwich Patch* – (Connecticut) **Offices remain closed as investigation of Greenwich haz mat incident continues.** Two town hall offices remained off limits to the public and to employees April 30 as local, State, and federal investigators continued their efforts to determine who left a powder-filled envelope in Greenwich Town Hall in Greenwich, Connecticut, April 26. An official said tests continued to determine the nature of the substance found in an envelope in the ground floor offices of the town's IT and GIS offices. The discovery led to a full-scale response by the Greenwich Fire Department, the Stamford Police Bomb Squad, the Connecticut Department of Emergency and Environmental Protection, and the FBI. The official said the GIS and IT offices remained closed through at least April 30. He also said the incident — which sent one Greenwich police officer to the hospital for evaluation after he was decontaminated at the scene — was prompting a review of security and access to the building. He said police officials will review whether there should be surveillance cameras to monitor who enters the building or a more strict access policy. Crews remained on the scene April 26 for about 5.5 hours.
Source: http://greenwich.patch.com/articles/investigation-of-greenwich-haz-mat-incident-continues

36. *April 29, Associated Press* – (Alabama) **University of South Alabama lockdown: Campus lockdown lifted hours after armed robbery.** The University of South Alabama in Mobile, Alabama, lifted a campus lockdown April 29 that it had imposed following an armed robbery at a college dorm hours earlier. University officials announced on their Web site that campus police arrested one male suspect and were searching for another in the robbery at gunpoint of a student. The victim invited the men to his room then they robbed him of $1,000 and a cell phone and fled, the statement said. A shot was fired. Officials believed the second robber left campus. Neither suspect apparently attended the school. The Mobile campus sent out an alert advising students to stay indoors after receiving a report of an armed robbery at the Delta 4 residence hall. Officials announced 4 hours later the lockdown was lifted and an arrest was made. The school used loud speakers, e-mails, and a dial-in phone system to advise students to seek shelter and stay indoors.
Source: http://www.huffingtonpost.com/2012/04/29/university-of-south-alabama-lockdown-robbery_n_1463248.html

37. *April 27, Myrtle Beach Sun News* – (South Carolina) **Horry County Schools faces fourth bomb threat of week.** Horry County Schools in South Carolina logged its fourth bomb threat of the week April 27, the 16th in a string of threats in 2012. The April 27 incident resulted in a 2-hour evacuation of Green Sea Floyds Middle and High School after a bomb threat was found in a girls' bathroom. Bomb threats also were found at Socastee High School April 24 and at Carolina Forest High School April 25 and April 26. Six people, including four juveniles, were charged in connection with the April 25 incident. The increase in threats prompted schools officials and police to work on public service announcements aimed at trying to deter additional instances.

Source: http://www.myrtlebeachonline.com/2012/04/27/2798266/horry-county-schools-faces-fourth.html

For more stories, see items **30**, **40**, and **48**

[Return to top]

Emergency Services Sector

38. *April 30, WAOI 4 San Antonio* – (Texas) **No water found in hydrants during apartment fire.** When firefighters responded to a fire April 29 that eventually destroyed 8 apartments and displaced 18 people in San Antonio, the firefighters were forced to search beyond nearby hydrants as two of the first hydrants were dry. The fire department plans to get to the bottom of why the hydrants were dry. They will look into who is in charge of the hydrants: the city or a private owner. If it is the city the fire department runs inspections and the San Antonio Water System makes repairs. Hydrant inspections happen about once a year.
Source: http://www.woai.com/mostpopular/story/No-water-found-in-hydrants-during-apartment-fire/dFxSgcLrxkSGbldqJztE_A.cspx

39. *April 30, KJRH 2 Tulsa* – (Oklahoma) **Lightning strikes sheriff's office, knocks out radio communications.** Lightning struck Oklahoma's Pittsburg County Sheriff's Office April 30, knocking out their primary radio communications. A backup system was used. As of 9:42 a.m. April 30 there was no estimate on how long the main system would be down, but officials said the outage had no effect on the performance of the office.
Source: http://www.kjrh.com/dpp/news/state/lightning-strikes-sheriffs-office-knocks-out-radio-communications

40. *April 28, Softpedia* – (Florida) **AntiSec hackers steal 40 GB of data from Lake County Sheriff's Office.** Softpedia reported April 28 a massive 40 gigabytes worth of files were stolen by Anonymous hackers operating under the AntiSec banner from the internal networks of the Lake County Sheriff's Office (LCSO) in Florida. One of the hackers that participated in the operation told Softpedia that out of the 40 gigabytes of data, around 35 gigabytes represent forensic software and other applications used by law enforcement agencies. The other 5 gigabytes are made up of reports that detail LCSO operations such as Op Inmate Intelligence Gathering and Operation Screen Savers. The files also include corporate security IPDR reports from Sprint Nextel that show the telecoms firm hands over private data to the authorities. Phone lists that reveal financial crimes, intelligence bulletins from the FBI, communication codes, and communications equipment are all contained in the data dump. Furthermore, hackers leaked the locations of U.S. Army Reserve facilities, badge numbers, 9-1-1 calls, log-in credentials, manuals, and official bulletins from the Department of Justice.
Source: http://news.softpedia.com/news/AntiSec-Hackers-Leak-40-GB-of-Data-from-Lake-County-Sheriff-s-Office-266784.shtml

41. *April 28, York Dispatch* – (Pennsylvania) **Former fire co. official guilty of embezzlement.** A former president of Lewisberry Community Fire Co. in York County, Pennsylvania, admitted to embezzling more than $11,000 from the company, which was forced to close because of financial debt, the York Dispatch reported April 28. She pleaded guilty April 19 to theft by unlawful taking, theft by failure to make required disposition of funds, and access device fraud. There is a second theft case against a co-defendant, a former Lewisberry fire chief. He has a pretrial conference scheduled for May 3. "They essentially financially destroyed that fire company," a local police chief said. A third official was also charged: Newberry Township Police filed a charge of criminal mischief against the fire company's last president. Police said he is responsible for building damage that allegedly happened in November 2011 as he and other members tried to move large appliances and other items from the station.
Source: http://www.yorkdispatch.com/news/ci_20493649/former-fire-company-official-guilty-embezzlement

42. *April 27, Athens Banner-Herald* – (Georgia) **Athens-Clarke police resolve 911 glitch.** The Athens Banner-Herald reported April 27 technicians resolved a recent glitch in the 9-1-1 system that prevented dispatchers at Georgia's Athens-Clarke County's 9-1-1 center from hearing the voices of people who used land lines to call in emergencies, according to an Athens-Clarke County police department news release. After discovering the glitch, the 9-1-1 center notified the telephone provider of the error. The company quickly corrected the problem that appeared to be limited to calls placed with land lines within Athens-Clarke County, police said.
Source: http://onlineathens.com/local-news/2012-04-27/athens-clarke-police-resolve-911-glitch

43. *April 27, Riverside Press-Enterprise* – (California) **Crews fix phone service in Running Springs.** Emergency 9-1-1 service for land lines in the Running Springs, California area was restored after a Verizon fiber optic was cut, according to the San Bernardino County Sheriff's Department. Running Springs residents were asked to use their cell phones to call 9-1-1 for emergencies, according to an e-mail from sheriff's officials who issued the advisory April 27. Four hours later, the department issued an update stating the line was repaired and emergency services were restored.
Source: http://www.pe.com/local-news/san-bernardino-county/san-bernardino-county-headlines-index/20120427-running-springs-line-cut-disrupts-emergency-calls-from-land-lines.ece

[Return to top]

Information Technology Sector

44. *April 30, Computerworld* – (International) **Down but not out: Conficker camouflages new Windows infections.** Windows PCs infected with Conficker are more likely to be compromised by other malware because the worm masks secondary infections and makes those machines easier to exploit, a security expert found. That is the biggest reason why Conficker, although crippled and seemingly abandoned by its makers, remains a threat and should be eradicated, a senior technologist at Neustar and a

cybersecurity adviser to the White House said. Neustar is an information and analytics provider, and one of the corporate members of the Conficker Working Group (CWG), which has been "sinkholing" the Conficker botnet for more than 2 years. The week of April 23, Microsoft said Conficker infected, or tried to infect, 1.7 million Windows PCs in 2011's fourth quarter. Microsoft called on users to strengthen passwords to stymie the malware. Conficker provides the cover the researcher spoke about because of two defensive tactics designed to keep it alive: the worm disables most antivirus software, including Microsoft's Windows Defender and Security Essentials, and switches off Windows' Automatic Updates, the service used by virtually all Windows users to keep their PCs patched. It also blocks access to security product Web sites — preventing signature updates for antivirus software — and to the Windows Update Web site. Without antivirus software, Conficker-infected systems are unlikely to detect and deflect other malware. If Automatic Updates is disabled, the machine will not receive any new security patches from Microsoft, leaving it open to attack by new threats that exploit those underlying vulnerabilities.
Source:
http://www.computerworld.com/s/article/9226697/Down_but_not_out_Conficker_camouflages_new_Windows_infections?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+computerworld/s/feed/topic/17+(Computerworld+Security+News)&utm_conte

45. *April 30, Help Net Security* – (International) **Gamex trojan threatens Android users.** A new Android trojan that paves the way for the download of other applications has been spotted on third-party Web sites, camouflaged as legitimate file managing, ad blocking, and performance boosting apps. According to Lookout researchers, the Gamex trojan's functionality is split across three components. Once the downloaded app repackaged with the trojan is granted root access by the user, the malware takes advantage of this permission to install another app onto the device, which then functions as a privileged installation service. "A third component communicates with a remote server, downloads apps, and triggers their installation. Gamex also reports the installation of these applications, along with the IMEI and IMSI, to a remote server," researchers explained. "We believe that this information is used to operate and/or report installations to a malicious affiliate app promotion network."
Source: http://www.net-security.org/malware_news.php?id=2086&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HelpNetSecurity+(Help+Net+Security)&utm_content=Google+Reader

46. *April 30, Softpedia* – (International) **Cybercriminals control Android TigerBot via SMS.** At the beginning of April, security researchers found a number of Chinese Android stores were pushing applications that masked a piece of malware called TigerBot (ANDROIDOS_TIGERBOT.EVL). Also known as Spyera, the malicious element was analyzed by Trend Micro experts. They discovered the malware was controlled by its masters via SMS or phone calls, being capable of performing a number of tasks, including call recording and GPS tracking. The list of commands accepted by TigerBot includes DEBUG, CHANGE_IAP, PROCESS_LIST_ADD, PROCESS_LIST_DELETE, ACTIVE, and DEACTIVE.

Source: http://news.softpedia.com/news/Cybercriminals-Control-Android-TigerBot-Via-SMS-267066.shtml

47. *April 29, Computerworld* – (International) **Snow Leopard users most prone to Flashback infection.** Of the Macs infected by the Flashback malware, nearly two-thirds are running OS X 10.6, known as Snow Leopard, a Russian antivirus company said April 27. Doctor Web, which earlier in April was the first to report the largest-ever malware attack against Apple Macs, mined data it intercepted from compromised computers to develop its findings. The company, along with other security vendors, has been "sinkholing" select command-and-control domains used by the Flashback botnet — hijacking them before the hackers could use the domains to issue orders or update attack code — to estimate the botnet's size and disrupt its operation. April 27, Doctor Web published an analysis of communications between 95,000 Flashback-infected Macs and the sinkholed domains. Those communication attempts took place April 13. Flashback uses a critical vulnerability in Java to worm its way onto Macs. Although Apple, which continues to maintain Java for its OS X users, patched the bug in early April, it did so 7 weeks after Oracle disclosed the flaw when it shipped Java updates for Windows and Linux. Sixty-three percent of Flashback-infected machines identified themselves as running OS X 10.6, or Snow Leopard, the newest version of Apple's operating system that comes with Java. Snow Leopard accounted for the largest share of OS X in March, according to metrics company Net Applications, making it the prime target of Flashback.
    Source: http://www.computerworld.com/s/article/9226696/Snow_Leopard_users_most_prone_to_Flashback_infection?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+computerworld/s/feed/topic/17+(Computerworld+Security+News)&utm_content=Google

48. *April 28, Ars Technica* – (International) **Backdoor that threatens power stations to be purged from control system.** Mission-critical routers used to control electric substations and other critical infrastructure are being updated to remove a previously undocumented backdoor that could allow vandals to hijack the devices, manufacturer RuggedCom said April 27. The announcement by the Ontario, Canada-based company comes 2 days after Ars Technica reported the company's entire line of devices running its Rugged Operating System contained a backdoor with an easily determined password. The backdoor, which cannot be disabled, had not been publicly acknowledged by the company until now, leaving the power utilities, military facilities, and municipal traffic departments using the industrial-strength gear vulnerable to sabotage that could affect the safety of huge populations of people.
    Source: http://arstechnica.com/business/news/2012/04/backdoor-that-threated-power-stations-to-be-purged-from-control-system.ars

For more stories, see items **5**, **8**, **33**, **49**, **50**, and **52**

To report cyber infrastructure incidents or to request information, please contact US-CERT at sos@us-cert.gov or visit their Web site: http://www.us-cert.gov

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: https://www.it-isac.org

[Return to top]

Communications Sector

49. *April 29, WHAM 13 Rochester* – (New York) **Time Warner Cable service restored in Rochester area.** Time Warner Cable restored service to customers in the Rochester, New York area after an extended outage April 29. A representative with Time Warner Cable said Internet and television services were back on as of 3 p.m. An equipment failure around 8 a.m. knocked out service to the area. Some businesses and restaurants reported having trouble running credit cards as a result of the outage.
Source: http://www.13wham.com/news/local/story/Time-Warner-Cable-Service-Restored-In-Rochester/emg55cuyzEqo1N0lxy8Uew.cspx

50. *April 29, Columbia State* – (South Carolina) **Time Warner Cable crashes Sunday afternoon; Columbia customers affected.** Thousands of Time Warner Cable television, telephone, and Internet customers in the Columbia, South Carolina area lost their connections for more than an hour April 29, a spokeswoman said. A large power outage of unknown origin took place at one of Time Warner Cable's main stations that feeds the Columbia area. "Typically, our backup power switches on and this isn't an issue," the spokeswoman said. "But in this case, when it switched on, we experienced a glitch, and it just took the services down." All Time Warner services — basic cable, digital cable, digital telephone, and high-speed Internet — were interrupted, she said.
Source: http://www.thestate.com/2012/04/29/2256023/time-warner-cable-crashes-sunday.html

51. *April 27, LaSalle News Tribune* – (Illinois) **Electrical fire sets back Catholic radio station.** An electrical fire knocked an Illinois religious radio station off the airwaves April 27. Standard Fire Department was called to a grass fire, the chief said. Firefighters from Standard and Cedar Point did not see signs of fire near the farmhouse at the given address but eventually located hot spots below a radio tower. A fire began sometime overnight within an insulated metal building containing electrical equipment for the tower, the chief said. The building was already nearly burnt out by the time firefighters arrived. A dry chemical was used on the building to suppress hot spots to protect any electronics that were still functional, the chief explained, but water was used to extinguish any burning grass and wood. The tower is owned by Nexstar and leased by WSOG 88.1 FM Spring Valley, a listener-supported Catholic radio station. The station's Web site reported it would be off the air for the "foreseeable future," but an online stream was still available, the station' operations manager said. He said he hoped to be back on the air in a few weeks, but it could take a few months to replace the equipment. The fire chief said the fire could have resulted from an electrical short

or from an animal chewing on wires.
Source:
http://newstrib.com/main.asp?SectionID=2&SubSectionID=27&ArticleID=18962

52. *April 27, Youngstown Vindicator* – (Ohio) **Thieves disrupt telephone and Internet service to hundreds in Warren today.** The theft of 2 60-foot cables strung on utility poles disrupted telephone and Internet service to up to 500 businesses and residents in the northwest quadrant of Warren, Ohio, for much of April 27. A Century Link representative contacted the Warren Police Department about the theft, saying it occurred sometime overnight. The cost to replace the cables, which were 1.5- to 2-inches in diameter will be about $10,000, officials estimated. Because of the cost of the cable, the theft was entered into the report as felony theft, and because of the effect on customers, it was also entered in as a disruption of public services.
Source: http://www.vindy.com/news/2012/apr/27/thieves-disrupt-telephone-and-internet-service-hun/?nw

For more stories, see items **29**, **40**, **45**, and **46**

[Return to top]

Commercial Facilities Sector

53. *April 30, Associated Press* – (Missouri) **St. Louis tent collapse raises safety questions.** St. Louis officials are expected to more closely scrutinize the large tents commonly set up near downtown stadiums after one of the temporary structures collapsed in high winds April 28, resulting in the death of an Illinois man and dozens of injuries after a baseball game. A spokesman for the city's mayor said it was unclear if adequate regulations were in place and being followed or if the disaster was simply the result of people not paying attention to severe weather warnings. The fast-moving storm ripped a large beer tent at Kilroy's Sports Bar from its moorings and sent it and debris hurtling through the air about 80 minutes after the end of a St. Louis Cardinals Major League Baseball game. Seventeen people in the tent were taken to hospitals, and up to 100 of the 200 gathered were treated at the scene, which was near Busch Stadium.
Source: http://www.weather.com/outlook/weather-news/news/articles/st-louis-tent-collapse_2012-04-28

54. *April 30, Duluth News Tribune* – (Minnesota) **Edge waterpark in Duluth to install new equipment to prevent waterborne illness.** Following an outbreak of cryptosporidiosis in March, the owners of the Edgewater Resort and Water Park in Duluth, Minnesota, are making a $100,000 investment in equipment to prevent future outbreaks, the Duluth News Tribune reported April 30. The park is installing an ultraviolet water-treatment system that will quickly eliminate harmful micro-organisms and bacteria from the water. Dozens of cases of cryptosporidiosis were traced to the water park, costing the business around $500,000 in lost business and new filtering equipment.
Source: http://www.duluthnewstribune.com/event/article/id/230170/

55. *April 29, Harrisburg Patriot-News* – (Pennsylvania) **East Hanover Township antique shop destroyed by fire; state police investigating.** A State police investigator was called to determine what caused a fire that destroyed a three-story antique shop April 29 in East Hanover Township, Pennsylvania. More than 20 fire companies from four counties responded. The lack of hydrants in the rural area made fighting the fire difficult, according to a Grantville Volunteer fire chief. Tanker trucks were used to bring in water. Firefighters had the fire under control in a few hours but remained at the scene for around 11 hours putting out hot spots.
Source:
http://www.pennlive.com/midstate/index.ssf/2012/04/east_hanover_township_antique.html

56. *April 28, Minneapolis Star Tribune* – (Minnesota) **Fire guts grocery, apartment building in Minneapolis.** A fire destroyed a Minneapolis neighborhood grocery store and left tenants of three upstairs apartments homeless, April 28. The fire started in the basement and quickly spread through the building. Firefighters had to leave when the structure became unstable. They were later forced to leave the interior as the west side of the building collapsed, and the fire began to burn the roof. One firefighter was taken to a hospital with an ankle injury. Fire officials said that what remained of the structure would have to be demolished.
Source: http://www.startribune.com/local/minneapolis/149356635.html

For more stories, see items **7**, **27**, **38**, **49**, and **52**

[Return to top]

National Monuments and Icons Sector

Nothing to report

[Return to top]

Dams Sector

57. *April 28, Spokane Spokesman-Review* – (Idaho; Washington) **Five rivers at flood stage in region.** Emergency management officials in north Idaho said April 27 the rush of water from mountain rain and snowmelt was stopping short of serious flooding. Levees and sandbags were holding at vulnerable locations as the rush of runoff neared its crest. The peak torrent was moving into Lake Coeur d'Alene and headed downstream to Spokane, Washington. Five of the region's rivers, including the Spokane, were at flood stage April 27. Lake Coeur d'Alene was expected to reach minor flood stage by dawn April 28 and crest late April 29 about 8 inches above flood stage. The director of emergency management in Benewah County, Idaho, said levees around St. Maries were holding despite pressure from the flooding St. Joe River. Seepage was spotted in several areas. The U.S. Army Corps of Engineers slowed the outflow from Libby Dam to keep the Kootenai River at Bonners Ferry below flood stage. Also, Albeni Falls Dam on the Pend Oreille River near Newport was opened to

allow more water to flow out of Lake Pend Oreille to protect property.
Source: http://www.spokesman.com/stories/2012/apr/28/five-rivers-at-flood-stage-in-region/

58. *April 28, Canadian Press* – (International) **Flash-flood fears subside as evacuation order lifts in Okanagan.** The risk of flash floods appeared to have lessened in the Naramata area west of Chuke Lake, British Columbia, Canada, where an evacuation order was lifted April 28. A spokesman for the Regional District of Okanagan-Similkameen said water levels above a dam dropped to about 8 inches April 28 after a high of about 28 inches April 27 when the order was issued for 46 homes. Water flow to a deteriorating forestry road was the major concern, said another district spokesman. Heavy rainfall was replaced by sunshine, but that could mean faster snowmelt for the community depending on how dry the weather gets, he said.
Source: http://www.theglobeandmail.com/news/national/fear-of-dam-burst-prompts-bc-evacuation/article2416863/?utm_medium=Feeds:RSS/Atom&utm_source=Home&utm_content=2416863

[Return to top]

Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Web site: http://www.dhs.gov/IPDailyReport

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703)387-2267
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer